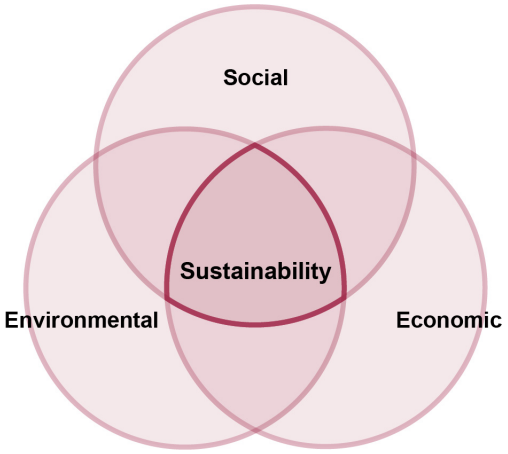
A few caveats apply here.

- **Board structure, objectives, and dynamics.** A board may want to consider whether internal audit involvement would be beneficial and acceptable, with appropriate safeguards to preserve internal auditor objectivity and independence.
- **Awareness of governance requirements.** Internal auditors could also take a proactive role in assisting the board with current governance obligations and practices. This could be accomplished by developing networks and processes to maintain awareness of these requirements and working with business round tables, professional trade associations, internal and external subject matter experts, and internal compliance or risk assessment committees. Auditors would then be prepared to assess:
  - Whether the organization is in compliance.
  - The ramifications of noncompliance.
  - The adequacy of the disclosures relating to the organization's governance system in its annual report.
- **Board education and training.** Internal auditors can assist the board in these efforts by developing and delivering training and providing related administrative support.

Topic D: Corporate Social Responsibility (Level B)

Corporate social responsibility (CSR), sometimes also called social responsibility (SR) or sustainable development (SD), is defined by *Sawyer's* as "the term commonly associated with the movement to define and articulate the responsibility of private enterprise for nonfinancial performance." The impetus for CSR owes much to another term, **triple bottom line,** which was popularized in 1994 by author and sustainability advocate John Elkington in his book *Cannibals with Forks: Triple Bottom Line of 21st Century Business.* The triple bottom line refers to the concept that corporate success should be measured in three dimensions—economic, social, and environmental—not just by the traditional economic bottom line of profitability. Exhibit V-10 illustrates how these dimensions overlap to create an organization that is sustainable over the long term.

Exhibit V-10: The Triple Bottom Line and Sustainability



Elkington wrote that these three areas must be fully integrated into the organization's business model and strategy to create organizational sustainability over the long term. Economic sustainability requires reinvestment of profits toward the growth of customer markets as well as investing in and tracking the impact of investments in environmental and social programs. This tracking and reporting process allows the social bottom line and the environmental bottom line to be measurable. Measurable results allow the long-term benefits of the programs to be measured against their costs so that better decisions can be made regarding which programs are truly contributing to the organization's sustainability. Such a tracking process can also allow the organization to market its successes.

Corporate social responsibility incorporates these concepts and ideals.

Understanding Corporate Social Responsibility

CSR has some alternate definitions in addition to the one provided above. The IIA Practice Guide "Evaluating Corporate Responsibility/Sustainable Development" states that:

> Generally, CSR is understood to be the way firms integrate social, environmental, and economic concerns into their values, culture, decision making, strategy and operations in a transparent and accountable manner and thereby establish better practices within the firm, create wealth, and improve society.

This definition underscores the importance of integrating CSR into the very fabric of the organization if it is to be successful, as was mentioned previously for the triple bottom line. CSR is a philosophy that must be championed from the top down. In fact, the board of directors is responsible for the effectiveness of CSR governance, risk management, and associated internal control processes. Senior management is responsible for establishing the objectives of CSR, managing related risks, measuring performance, and monitoring and reporting on CSR issues. However, one tenet of CSR is that, like TQM (total quality management), everyone at an organization has a role to play in ensuring the fulfillment of CSR objectives. Therefore, thorough change management is needed to ensure that these objectives are reinforced and brought into the culture and incentive structures of the organization.

Some organizations, such as those that have little direct impact on the environment, will define the objectives of CSR a little differently, making the environment just one element of CSR and emphasizing other social objectives more, such as ethics and transparency, donations and political contributions, corporate/organizational governance, human rights, human resources and employment, supply chain management, shareholder relations, health and safety, and community investment.

Stakeholders to CSR and Their Needs

Exhibit V-11 lists a number of stakeholders to the CSR process, reprinted from The IIA's course "Corporate Social Responsibility: Opportunities for Internal Audit," although the "environment" stakeholder might be better termed as "supporters of the environment," since the environment cannot speak for itself.

Exhibit V-11: Stakeholders to CSR and Their Needs

Stakeholders	Needs
Employees (and their families)	Fair pay, living wage Respect (freedom from discrimination and harassment; equity) Support systems (education, social benefits) Safety and security
Environment	Clean air, water, land Recycle, reuse, reduce waste Respect for ecosystems and animals
Neighboring community	Philanthropy Capacity building Social welfare Economic opportunities
Shareholders	Transparency and honesty Longevity (sustainable) Reputation and legal compliance Optimization of return Governance Pursuit of strategy in ethical/legal fashion
Customers	Safety Transparency and honesty Optimization of price
Suppliers	Fair negotiations Relationships Contractual compliance

Each stakeholder has certain needs that if met, will reduce the risks to the organization (if the need can be met without undue hardship or expense).

Risks That CSR Is Intended to Address

The results of a risk management assessment will help identify a variety of risks, some of which can be managed using a CSR program and some of which will be created by the CSR program itself.

- **Strategic risks.** Strategic risks include having an inadequate or ineffective strategic decision-making process or control development process related to a CSR program. This could lead to poor results from approved projects or other initiatives, which could then result in less ability to get future CSR projects or initiatives approved.

- **Reputation risks.** An organization that fails to address the needs of its stakeholders (as defined previously) may earn a negative reputation. The saying that it takes years to build a reputation but just moments to destroy it is as true for organizations as it is for individuals. Damage to organizational reputation is hard to measure, but many organizations have lost market share or investor confidence or suffered other real effects from a poor reputation.

  Another risk to reputation is from the CSR program itself. The program usually involves publishing voluntary reports, which can be used to attract new investors and advertise the organization's successes, but they could also be used by environmental or social activists to level attacks on the organization. Even an effort in the right direction may not be seen as enough by some groups. The CSR program could also fail to be enacted or run properly, or breakdowns in controls could occur. Internal audits of CSR programs could objectively assess information provided in reports or determine the efficiency and effectiveness of CSR.

- **Compliance risks.** There are myriad laws and regulations under the purview of a CSR program, and, because of this, there are risks of noncompliance due to ignorance (which is not an allowed excuse) or deliberate actions. Organizations operating in multiple countries will experience a higher level of compliance risk.

- **Liability risks.** Liability risks can occur because an organization has not provided adequate controls to address a risk or because a risk event occurs, perhaps due to a control weakness or failure. Often, if an organization can prove that it had the proper controls in place, it can limit the damages even if there has been a control failure. For example, if an employee sues for sexual harassment but the organization can prove that it has a program in place to require managers to be trained on sexual harassment, in certain jurisdictions the organization may be able to show that it has established a "zero tolerance" atmosphere toward sexual harassment and reduce some of the damages (such as preventing the case from becoming a class action lawsuit).

Liability risk can also exist as part of the CSR program. If an organization's business partners are contractually required to follow certain CSR standards or policies, there is a risk of noncompliance and legal liability. Even if a supplier assumes all liability, it could create a supply chain disruption or worse. Independent or internal audits can help address this risk.

- **Operational risks.** An organization's operations may create air, water, or noise pollution, workplace hazards, or products that cause unintended harm to consumers. An organization can face these risks even if it is in full compliance with the laws and regulations of a country, especially if the country has relatively lenient laws or cannot or will not enforce its laws and regulations. This is because an organization's business practices in such countries could be brought to light and harm the organization's reputation or create direct liability risk.

  Operational risks can also be created by a CSR program. The CSR program may fail to meet its operational goals. The goals could be unrealistic, not address the highest priority risks, or be more expensive to implement than originally expected. The program could also fail because it is not integrated into business strategy or business processes or because adequate controls over CSR processes fail to be developed or implemented. Organizations adopting CSR standards or policies may face difficulty when attempting to apply them in different countries.

- **Reporting risks.** Improper or inaccurate financial or nonfinancial reporting about an organization's CSR program or its impact/results could lead to many other types of risks, such as reputation risk, compliance risk, or liability risk.

- **Staffing risks.** Employees and potential employees have expectations for their place of work such as fair pay and respect. Having a great CSR program may become one of these expectations if it is the industry norm. The organization may have difficulty attracting and retaining talent if it lacks such a program.

- **Marketing risks.** Closely associated with reputation risk, marketing risks can arise if the organization is not proactive in implementing or advertising a CSR program. This could include boycotts, missing out on a socially active customer segment, or simply losing market share to an organization that is actively engaged in CSR.

- **Supply chain partner risks.** Suppliers, business partners, and downstream customers in the supply chain, such as wholesalers, could act unethically (even if legally) if no contractual obligations exist, or they could violate CSR contractual terms and conditions and the organization could suffer from guilt by association. Monitoring controls may be difficult, especially for long distance relationships.

CSR Process

CSR starts with the board and senior management determining their priorities and high-level objectives. The next step is to identify and prioritize significant risks related to CSR. Management may adopt an external CSR framework such as ISO 26000 or the Global Reporting Initiative and/or translate these objectives into high-level policies.

Once a framework and policies are in place, the next step is to set detailed objectives, performance targets, and implementation strategies. Examples of objectives include reducing safety incidents, encouraging volunteerism, creating a culture of transparency, or reducing waste or carbon emissions.

A best practice is for organizations to embed CSR principles into their business processes to ensure that they occur, such as by engaging employees from the bottom up in crafting mission and vision statements that reflect CSR values, requiring a life-cycle value assessment of projects or product designs with the environment and social impact in mind, or requiring that CSR risks be assessed and addressed prior to allowing project approvals.

Once processes are developed, they must be managed and measured against performance targets or other benchmarks. Results are analyzed and recommendations are made to complete the cycle of continual improvement. For example, the organization's emissions could be tracked and compared to industry benchmarks or internal goals. Product hazards could be verified and quantified using laboratory testing. Employee satisfaction could be measured using self-assessment tools. Commitments made to stakeholders could be reviewed to ensure that they were honored. Internal auditors may play a role at this point of the process.

One ongoing process throughout the CSR development life cycle is to regularly communicate with stakeholders. This may include involving stakeholders in policy development, distributing surveys and collecting feedback, forming focus groups, or managing the complaints process.

Another ongoing activity is internal and external auditing and compliance. Internal auditors test internal controls and CSR management systems. Compliance professionals may determine whether the organization and its supply chain partners are in compliance with laws, regulations, contracts, and policies, but internal auditors may be called upon to determine how effectively these processes are being conducted.

The final element in the CSR process is CSR reporting. CSR reporting is addressed later, but examples include voluntarily supplying information on carbon emissions, issuing safety data sheets for hazardous products, and making other required public disclosures and reports.

CSR Frameworks

Organizations may wish to adopt a CSR framework of policies and standards rather than developing them on their own. The use of a framework has many advantages, from providing a common vocabulary to easier adoption in various countries, especially when international standards are used. Common CSR frameworks include ISO 26000 and the Global Reporting Initiative.

ISO 26000:2010, "Social Responsibility"

ISO 26000:2010, "Social responsibility," provides guidance on:

- Terms, definitions, and concepts related to social responsibility.
- The characteristics of social responsibility, its background, and trends.
- Principles and practices related to social responsibility.
- The core issues and subjects of social responsibility.
- Integrating, implementing, and promoting socially responsible behavior throughout the organization and, through its policies and practices, within each area's sphere of influence (i.e., internal auditing for internal auditors).
- Identifying and engaging with stakeholders.
- Communicating commitments, performance, and other information.

ISO 26000 is intended to promote a common understanding of social responsibility among employees and encourage them to go beyond legal compliance. Motivated and empowered employees add value to programs and provide valuable word-of-mouth marketing within and outside the organization. This can help with CSR adoption and contribute to sustainable development.

Global Reporting Initiative

The Global Reporting Initiative (GRI) is a network-based organization that produces a reporting framework for sustainability actions and results. This reporting framework is subject to continuous improvement and has been widely adopted globally. GRI reports can be easily benchmarked against reports from other organizations using this framework. GRI also provides advice and standards on how to measure performance against key performance indicators.

CSR Reporting

CSR reports can be stand-alone or part of an organization's annual report. Selected CSR information could also be included in marketing releases such as brochures for shareholder meetings, web pages, commercials, or press releases. Regulators may also require that certain filings be made.

Reporting on CSR is important because these disclosures allow potential investors to determine if the organization qualifies as a socially responsible investment, open the organization to additional investor classes, or may provide information on whether the organization is sustainable in the long term per the triple bottom line discussion earlier. However, organizations need to carefully consider what to include and omit from such reports, not only because the information has a liability risk (e.g., being used by unfriendly activists) but also because the potential benefits of gathering that information must outweigh the costs of producing the information in the first place. An organization that embarks on CSR reporting must also recognize that it will sometimes need to share bad news as well as good. However, organizations that consistently report both positive and negative information will be considered more trustworthy.

Some countries such as France have laws requiring organizations to report on their environmental and social impact. Canada has a similar law requiring banks and federally incorporated trusts with more than $1 billion in equity to report their contributions to the economy and society. Similarly, the United Kingdom has rules for pension funds to report on the ethics and social and environmental policies of organizations in which they invest.

In addition to the challenge of determining what to include in a report, the report format and terminology used also pose challenges for the comparability of information reported. Unlike external financial reporting, which has been standardized to make statements fairly comparable, CSR does not yet have a generally accepted format for reporting. ISO 26000 or GRI could provide this common framework, but a critical mass of voluntary adopters will be required to make comparability a reality.

Another issue with CSR reporting is that reports may not be considered trustworthy unless they have been independently verified by third parties or have been subject to some other type of assurance process. Internal auditors are one possible resource that could provide this assurance. To complement such assurance processes, auditors or other assurance providers can use CSR assurance standards, such as those produced by AccountAbility, an international not-for-profit organization. Its AA1000 standard is a principles-based standard that provides methods of continually improving sustainability performance. An organization could also receive a certification that it is compliant with ISO 26000 or other relevant ISO standards. This requires submitting the organization to a review from an accredited third-party testing organization.

Auditing CSR

Corporate social responsibility encompasses a very broad range of organizational activities and related controls. Therefore, various elements of CSR will likely be audited on a cyclical basis. Some elements of CSR may require extended time to obtain sufficient audit evidence and can therefore only be audited after that point. Exhibit V-12 provides some possible methods of selecting CSR elements to audit.

Exhibit V-12: Methods of Auditing CSR

Audit Method	Description
Audit by element	Perform separate audit engagements for each CSR element, such as governance; environment; ethics; community involvement; health, safety, and security; transparency; and working conditions and human rights. Engagements can subdivide elements by business location or external partner.
Audit by stakeholder	Perform separate audit engagements to assess effectiveness of delivering value to each stakeholder group such as employees and their families, customers, the environment, and so on. The basis for determining effectiveness is fulfillment of each group's needs. Each engagement could be subdivided by location or external partner.
Audit by common subject	Perform audits by common subject area, such as workplace, marketplace, community, and environment. Auditing by workplace could bundle issues together such as employer of choice, health and safety, diversity and equality, environmental management practices, training and development, ethics, governance, and human rights. In another example, bundling by community could include assessing local economic support, charity, capacity building, volunteerism, and stakeholder engagement.
Audit by internal control	Perform audits using internal controls over risk management, data gathering, measuring, and CSR reporting activities for each department or organizational group to be audited in the audit plan. The same audit tests would be performed for each area so the results would be comparable. At the end of the year, an overall report on CSR could be made based on all areas audited.
Audit by risk-management-based priority	Perform audits using a risk-management-based approach, selecting the areas of a CSR program identified as being most significant in terms of risk impact and likelihood, with direction provided by board and senior management. This method can be combined with any of the prior methods.

There are other related audit topics in which the CAE could serve as a project manager or an internal auditor could be used as a resource if managed by another area:

- Auditing public disclosures about the organization's CSR approach and results to provide assurance that the results are reliable
- Auditing third parties for contractual compliance with CSR terms and conditions or reviewing prospective suppliers to prequalify them

The CAE must assess his or her audit team's capabilities to perform CSR audits and consider adding external subject matter expertise when needed. For example, internal auditing may need to use a management self-assessment process to audit some CSR controls or results. It is essential that internal auditors possess good facilitation skills when explaining how to perform self-assessments and when providing feedback on results. Internal auditors also need adequate communication skills to carefully address sensitive issues such as ethics or working conditions. The IIA's Certification in Control Self-Assessment is one way to ensure that audit staff have the proper skill set for this activity.

There may also be situations in which the internal auditor is responsible for some aspect of a CSR program's operations. When this is the case, that portion of the program could be audited by an independent third-party service provider.

CSR auditing engagements could also be performed as consulting engagements, in which case the internal auditor could provide input during the design phase of CSR programs to ensure that proper controls are developed and integrated seamlessly into processes.

Topic E: Risk Management Fundamentals (Level P)

What Is Risk Management?

The *Standards* Glossary defines **risk management** as "a process to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives."

On one level, all employees—including internal auditors—are risk managers, whether they know it or not. They manage risks every day to help them achieve their goals and objectives. But they become better risk managers when they do it consciously, in a disciplined and consistent way.

From the organization's standpoint, great benefits can be derived if managers do not just manage their own risks within their own organizational "silos." If the same disciplined risk assessment process is applied throughout the organization and the results are rolled up to higher levels, executive management can see the total picture of risk for the organization. With this "portfolio view" of risk in mind, executives can make better strategic decisions and allocate resources more effectively.

Organizations around the world are developing enterprise risk management (ERM) programs to realize these benefits. Our discussion of risk management will focus on ERM, which encompasses all risk management concepts.